PHISHING, SMISHING Y PHARMING EN EL PROCESO PENAL ARGENTINO

Tipicidad, prueba digital, autoría y límites constitucionales en la investigación de fraudes bancarios

Jacobo Iván Selser · 29/01/2026

I. Introducción

El fraude digital como problema jurídico (no solo tecnológico)

El crecimiento exponencial de los fraudes bancarios digitales ha colocado al proceso penal frente a un desafío que no es meramente técnico, sino dogmático y constitucional. Términos como phishing, smishing y pharming circulan hoy en denuncias, dictámenes fiscales y resoluciones judiciales con una liviandad que contrasta con su impacto real en la estructura de imputación penal.

El problema no reside en la novedad del fenómeno, sino en la forma en que se lo aborda jurídicamente. La tendencia a utilizar estas categorías como rótulos genéricos —o peor aún, como sinónimos— conduce a investigaciones desordenadas, imputaciones imprecisas y, en última instancia, a procesos frágiles desde el punto de vista probatorio.

Este trabajo parte de una premisa clara: phishing, smishing y pharming no son delitos en sí mismos, sino modalidades de ejecución que inciden directamente en la tipicidad, en la prueba exigible y en la atribución de autoría. Confundir estas dimensiones equivale a abdicar del análisis penal riguroso.

II. Delimitación conceptual

Tres técnicas, tres problemas jurídicos distintos

1. Phishing

El phishing consiste en la obtención fraudulenta de credenciales de autenticación mediante engaño dirigido a una persona. Correos electrónicos, sitios web clonados, falsos contactos de atención al cliente o mensajes que simulan comunicaciones bancarias constituyen su expresión más conocida. Desde el punto de vista penal, el elemento decisivo es la interacción humana: la víctima, inducida en error, entrega voluntariamente el dato que habilita el acceso a su cuenta o instrumento financiero.

2. Smishing

El smishing reproduce la lógica del phishing, pero a través de SMS o mensajería instantánea. Su relevancia jurídica no está solo en el canal, sino en la volatilidad extrema de la prueba: mensajes

que se borran, funciones de eliminación remota, cambios de SIM, reemplazos de dispositivo. Esto convierte al smishing en una modalidad especialmente sensible desde la perspectiva de la cadena de custodia y la preservación temprana de evidencia digital.

3. Pharming

El pharming introduce un quiebre cualitativo. Aquí el engaño ya no se dirige primariamente a la voluntad de la víctima, sino a la infraestructura técnica: manipulación de DNS, redirecciones maliciosas, malware, control del router o del dispositivo. La consecuencia dogmática es inmediata: el foco del análisis se desplaza del error subjetivo a la vulneración técnica del sistema, con implicancias directas en la tipificación penal.

III. El iter típico del fraude bancario digital

De la captación de credenciales a la monetización

Más allá de la técnica empleada, la mayoría de los fraudes bancarios digitales responde a una secuencia relativamente estable: captación del factor de autenticación (credencial, token, código de verificación), acceso a la cuenta o instrumento financiero, operación (transferencias, compras, préstamos, alta de beneficiarios), monetización (cuentas puente, "mulas", criptoactivos, comercios pantalla) y ocultamiento (borrado de mensajes, modificación de alertas, dispersión de fondos).

Esta estructura es clave porque permite desagregar conductas. No siempre quien obtiene la credencial es quien opera la cuenta, ni quien recibe el dinero es quien participó del engaño inicial. Ignorar esta fragmentación conduce a imputaciones expansivas y endebles.

IV. La batalla de la tipicidad

Art. 172 CP vs. art. 173 inc. 16 CP

Uno de los errores más frecuentes en la práctica forense es tratar todos los fraudes digitales bajo un único encuadre típico. Sin embargo, la distinción entre estafa clásica y defraudación informática no es meramente académica: tiene consecuencias prácticas decisivas.

1. Estafa (art. 172 CP): engaño a la persona

Cuando el núcleo del hecho reside en la ingeniería social —esto es, en un engaño dirigido a una persona que entrega voluntariamente la credencial— el encuadre natural es el de estafa. El error de la víctima es el motor causal del desplazamiento patrimonial.

2. Defraudación informática (art. 173 inc. 16 CP): vulneración técnica

Cuando, en cambio, el resultado se produce mediante manipulación técnica del sistema, sin interacción humana directa relevante (pharming "silencioso", malware, redirecciones automáticas), el eje se desplaza hacia la defraudación informática incorporada por la Ley 26.388.

Esta distinción no es retórica: cambia la descripción del hecho, modifica el enfoque probatorio, incide en la estrategia de imputación y defensa, y condiciona la discusión sobre concursos y autoría. Presentarla como criterio de orientación —y no como regla automática— permite ordenar el análisis sin forzarlo.

V. Prueba digital

Entre la abundancia y la fragilidad: el espejismo de las capturas de pantalla

En las causas por fraude digital, el expediente suele "llenarse" de prueba rápidamente: capturas de pantalla, resúmenes bancarios, listados de operaciones. El problema es que la cantidad no sustituye a la calidad.

Las capturas de pantalla, por sí solas, carecen de garantía de integridad (hash), trazabilidad de origen y contexto técnico verificable. Sirven para iniciar una investigación; no alcanzan para sostener una imputación penal. Cuando el proceso se apoya exclusivamente en ese tipo de material, el estándar probatorio se degrada peligrosamente.

En contraste, la evidencia de mayor valor —logs de acceso, registros de autenticación, huella de dispositivo, correlación temporal, eventos antifraude— suele llegar tarde, incompleta o directamente no llegar. Allí se juega, en serio, la robustez del caso penal.

VI. Identificación técnica y el problema de las IP

CGNAT y la falacia de la autoría automática

Un punto crítico en estos procesos es la identificación del autor a partir de direcciones IP. En el contexto argentino, esta práctica enfrenta un obstáculo técnico relevante: el uso extendido de CGNAT (Carrier Grade NAT) por parte de proveedores de internet.

Bajo este esquema, una misma IP pública puede ser compartida por múltiples usuarios en simultáneo. Sin la identificación del puerto de origen (source port) y la correlación temporal precisa, la IP no individualiza a una persona. Este dato técnico no invalida toda investigación basada en IP, pero obliga a una advertencia metodológica: la IP no es, por sí sola, una identidad penal. Tratarla como tal conduce a inferencias débiles y a imputaciones que no resisten el contradictorio.

VII. Autoría, participación y el dilema de la "mula"

El nudo real de los litigios actuales

Quizás el problema más delicado —y más frecuente— en estas causas sea la imputación al titular de la cuenta receptora de fondos. La fiscalía suele optar por la figura de partícipe necesario de la estafa. Sin embargo, esa calificación exige un análisis subjetivo riguroso.

En la práctica aparecen, al menos, tres hipótesis: (i) partícipe, con conocimiento y aporte doloso al fraude; (ii) encubridor (art. 277 CP), con intervención posterior al hecho principal; y (iii) sujeto instrumentalizado: "mula" captada mediante engaño (oferta laboral falsa, promesas de comisión), sin conciencia del origen ilícito.

Confundir estas categorías no es un error menor: implica imputar dolo donde puede haber error, o participación donde puede haber mera utilización. La dogmática penal exige resistir esa simplificación.

VIII. Smishing y mensajería digital

Cadena de custodia, volatilidad y preservación temprana

El smishing presenta un desafío probatorio específico: la extrema volatilidad de la mensajería. A diferencia del correo electrónico tradicional, los mensajes SMS o de aplicaciones de mensajería pueden eliminarse sin dejar rastro accesible al usuario, ser modificados por funciones de "eliminar para todos", o perderse por cambios de dispositivo, restauraciones o reemplazo de SIM.

Desde el punto de vista procesal, esto exige abandonar una práctica frecuente: incorporar al expediente reconstrucciones tardías presentadas como si fueran evidencia original. Una fotografía del teléfono o una transcripción posterior carecen de garantías mínimas si no se preservó el mensaje en su estado original y con trazabilidad verificable.

Aquí, la cadena de custodia no cumple una función meramente ordenadora: es la única forma de distinguir entre un mensaje efectivamente recibido en un momento determinado y una recreación posterior, incompleta o contaminada. En delitos digitales, lo que no se preserva a tiempo suele perderse para siempre.

IX. Pharming y prueba técnica

Cuando el expediente exige pericia y no relato

El pharming obliga a un cambio de paradigma probatorio. A diferencia del phishing clásico, donde el engaño puede describirse desde la experiencia de la víctima, el pharming solo se acredita mediante explicación técnica.

No alcanza con afirmar que la víctima "ingresó al sitio correcto y fue redirigida". Es indispensable demostrar qué componente del sistema fue afectado (DNS, router, dispositivo o red), cómo se produjo la redirección, con qué alcance y persistencia, y qué relación guarda ese evento con el acceso posterior a la cuenta.

La ausencia de una pericia clara no es un defecto formal: impide reconstruir el hecho. Imputar pharming sin acreditación técnica es confundir una hipótesis con una prueba.

X. Cooperación internacional y la variable tiempo

Budapest como marco, no como salvación

En la mayoría de los fraudes digitales, algún tramo del hecho atraviesa fronteras: dominios registrados en el exterior, servidores remotos, proveedores de correo o mensajería, exchanges de criptoactivos. La Convención de Budapest, aprobada por Argentina mediante la Ley 27.411, ofrece un marco para la cooperación, pero no elimina un problema estructural: el tiempo.

La evidencia digital tiene una vida útil corta. Registros de sesión, logs de proveedores y datos de tráfico se conservan por plazos limitados. Cuando los requerimientos internacionales se cursan tarde o de manera imprecisa, la información ya no existe.

Desde una perspectiva garantista, este desfasaje no puede resolverse con presunciones. La imposibilidad material de obtener un dato no habilita a suplirlo con inferencias. La urgencia investigativa exige precisión temprana; su ausencia debilita el caso.

XI. Estafa bancaria y desconocimiento de cargos

El diálogo entre el proceso penal y el derecho del consumo

Muchos procesos penales por fraude digital se originan en un desconocimiento de cargos formulado por el cliente bancario. En sede civil o de consumo, ese acto activa deberes de investigación y seguridad a cargo de la entidad financiera. En sede penal, cumple una función distinta.

El desconocimiento de cargos no prueba por sí mismo la existencia de un delito ni identifica al autor. Sin embargo, genera un conjunto de datos relevantes: alertas internas del banco, evaluaciones de riesgo, decisiones automatizadas o manuales, registros de comportamiento atípico.

Ignorar ese material empobrece la investigación penal. Trasladarlo acríticamente, también. El desafío consiste en integrar la información bancaria como contexto, no como sustituto del estándar probatorio penal.

XII. Consecuencias procesales

Nulidad, exclusión y pérdida de fuerza convictiva

Las irregularidades en la obtención y preservación de evidencia digital no admiten soluciones tibias. Cuando la prueba se obtiene violando garantías constitucionales —por ejemplo, mediante accesos no autorizados, preservaciones defectuosas o reconstrucciones no verificables— la respuesta del sistema debe ser la exclusión.

En otros casos, el vicio puede no alcanzar el umbral de la ilicitud, pero sí afectar gravemente la confiabilidad del material. Allí la prueba puede subsistir formalmente, pero pierde fuerza

convictiva, especialmente si constituye el eje central de la imputación.

Aceptar imputaciones basadas en evidencia débil, incompleta o inferida implica degradar el estándar penal. Y esa degradación, lejos de fortalecer la persecución del fraude, termina debilitando la legitimidad del sistema.

XIII. Conclusión

Validar la evidencia antes de imputar

Phishing, smishing y pharming no son categorías de moda ni etiquetas mediáticas. Son técnicas de ejecución que exigen respuestas jurídicas diferenciadas. Tipificar correctamente, preservar evidencia de calidad, distinguir roles y respetar las garantías no es un obstáculo para la investigación penal: es su condición de posibilidad.

El proceso penal digital no puede construirse sobre capturas de pantalla tomadas como verdad revelada ni sobre inferencias técnicas simplificadas. La tecnología amplía las capacidades del delito, pero también eleva el deber de control del Estado.

Validar la evidencia antes de imputar no es una concesión a la defensa. Es una exigencia del Estado de Derecho. Allí donde ese control se relaja, el proceso deja de ser un instrumento de justicia y se convierte en una reacción improvisada frente a la complejidad tecnológica.

FUENTES Y REFERENCIAS (SELECCIÓN MÍNIMA)

Marco normativo, jurisprudencia, doctrina y estándares técnicos utilizados como soporte argumental y para notas al pie.

Marco normativo

Constitución de la Nación Argentina (arts. 18 y 19; y tratados con jerarquía constitucional, en particular CADH art. 11 y PIDCP art. 17).

Código Penal de la Nación: arts. 172 (estafa), 173 inc. 16 (defraudación mediante una técnica de manipulación informática), 153 bis (acceso ilegítimo a un sistema o dato informático) y 277 (encubrimiento), entre otros.

Ley 26.388 (Delitos Informáticos): reforma del Código Penal e incorporación/adecuación de tipos vinculados a sistemas y datos informáticos.

Ley 27.411 (Convenio sobre Ciberdelito del Consejo de Europa – Convención de Budapest): marco de cooperación y lenguaje técnico-jurídico (preservación rápida, datos de tráfico vs. contenido, etc.).

Ley 25.326 (Protección de Datos Personales): referencia tangencial relevante cuando la investigación requiere tratamiento de datos personales y su compatibilidad con legalidad y finalidad.

Código Procesal Penal de la Nación (CPPN) y Código Procesal Penal Federal (CPPF): reglas de obtención y control judicial de medidas de investigación; nulidades y contradicción.

Jurisprudencia

CSJN, “Halabi, Ernesto c/ P.E.N. – ley 25.873 – dto. 1563/04 s/ amparo ley 16.986”, Fallos 332:111 (privacidad, vigilancia masiva y control judicial efectivo).

CSJN, “Quaranta, Carlos Alberto s/ causa n.º 1132”, Fallos 333:1674 (deber de motivación y anulación de intervención por falta de fundamentos objetivos).

CSJN, “Montenegro, Luciano Bernardino s/ robo”, Fallos 303:1938 (límites a la prueba obtenida con violación de garantías).

CSJN, “Fiorentino, Diego”, Fallos 306:1752 (prueba ilegítima y doctrina de exclusión).

CSJN, “Rayford”, Fallos 308:733 (exclusión probatoria; regla de no aprovechamiento estatal de la violación).

CSJN, “N.N. s/ violación de sistema informático (art. 153 bis, primer párrafo, CP)”, 23/06/2015 (criterios de competencia y tratamiento del acceso ilegítimo a cuentas/servicios).

TSJ CABA, “Incidente de competencia en autos López, Diego Fernando sobre 173 incs. 15 y 16 – defraudación mediante el uso de tarjetas / defraudación informática – conflicto de competencia”, 23/11/2022 (delimitación típica y consecuencias en competencia).

Cámara Nacional de Casación en lo Criminal y Correccional, Sala 3 unipersonal, CCC 32757/2022/TO1/3/CNC1, Reg. 1792/2024, 17/10/2024 (declinatoria parcial de competencia en investigación por art. 173 inc. 16 CP; sentencia publicada por CIJ).

Doctrina y estándares técnicos (uso prudente)

Figari, Rubén E., “Reflexiones sobre la defraudación informática. Artículo 173, inciso 16, Código Penal”, doctrina (SAIJ).

Bieniauskas, Carlos A., reseña y análisis sobre “Phishing–Pharming: nuevas modalidades de estafas on line” (Monastersky & Costamagna), doctrina (SAIJ).

Hertler, F. E., “El convenio de Budapest y su influencia en el derecho penal argentino” (2024), artículo disponible en PDF (Pensamiento Penal).

ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition and preservation of digital evidence* (estándar técnico orientativo, citado habitualmente en literatura forense).

IETF RFC 6888, *Terminology for Carrier-Grade NAT*, y documentos conexos sobre correlación de IP/puertos/tiempo y requerimientos de logging en NAT a gran escala.